Module 1. Biometrics for Identifying People

Francesc Serratosa

Universitat Rovira i Virgili

Tarragona, Catalonia.

September 2018

francesc.serratosa@urv.cat

http://deim.urv.cat/~francesc.serratosa/

Introduction

Biometrics is a science that analyses the positions and distances between parts of our body to identify or classify people. There are several biometric features that are currently used, such as fingerprints, the face, iris, hands, the retina and the signature. Biometrics, and more specifically fingerprints, were first studied at the end of the nineteenth century in forensic applications for identifying criminals or obtaining people's identity. Today, not only is biometrics used in these applications but also in others, like controls at airports, access to nuclear power stations or military installations, or even simply access to offices or municipal swimming pools. Biometrics is becoming part of our daily lives and it is necessary that computer scientists and engineers in general have at least a basic knowledge of it.

To increase the reliability of biometric systems, some applications use several biometric features together. For example, merging ear recognition with gait (the way of walking) recognition is currently under study. This is because these two techniques can be applied in similar situations. Video cameras can record people walking without user collaboration. This merging of methods is not always easy. However, despite its importance, due to time limitations we will not discuss merging biometric systems here.

This didactic module is the first of the subject *Biometrics* imparted at Universitat Rovira i Virgili (Tarragona, Catalonia). The purpose of which is to outline the main aspects of biometric techniques. To understand it, you do not need to go deeper into the following modules as the aim is that it is self-contained. Module 2 looks at analysing the errors in real biometric systems and also gives examples of large-scale biometric applications. Modules 3, 4 and 5 are devoted to the verification and identification of individuals with the most commonly used techniques: fingerprints, the face and iris, respectively. Finally, Module 6 looks at the security of biometric systems. The ultimate goal of incorporating biometric systems into another system is to increase the security of this second system. Therefore, it is important to ensure that the biometric system itself does not have errors through which the security of the entire system could be compromised.

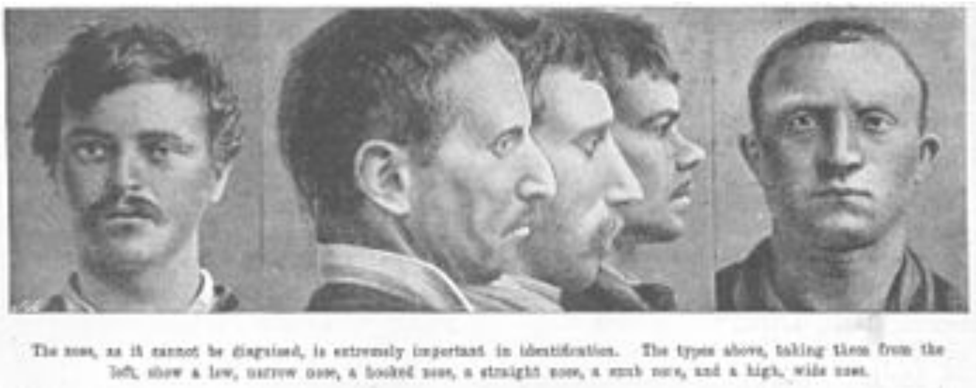
Objectives

This module is the first module of the *Biometrics* subject. The objectives are to explain the basic foundations of biometrics used for identifying people, as well as introduce the concepts and terminology that will be used in the following modules:

- Introduce the effectiveness and necessity for biometrics in today's society.
- Define the characteristics a biometric feature needs to be used in specific applications.
- Classify the biometric features that can be used to identify and verify people.
- Formulate and describe the stages or internal processes of the three basic biometric systems: Identification, Verification and Enrolment.
- Classify errors that may appear in a biometric system and define in which conditions these errors appear.
- Evaluate a biometric application to determine its goodness: Metrics to evaluate and compare the goodness of the biometric systems.
- Classify the different applications in which biometric techniques can be used to ensure or increase their security.
- Brief history of biometrics used for identifying and verifying people.
- Comment on how the cinema and art worlds have featured and used biometrics.
- Discuss the possible violation of people's identity and comment on ethical problems.

1 The Beginnings

In 1882, the French police officer **Alphonse Bertillon** (1853-1914) presented the first system for identifying people based on physical characteristics, that is, on biometric features. He called it *Anthropometry* and it is considered the first scientific system used by police to identify criminals. Initially, the system aimed to classify people's nose, face or body shape. Figure 1 shows an illustration published in *Pearson's Magazine*, Volume XI (January 1901), showing different nose classes defined in anthropometry.



1. Illustration published in *Pearson's Magazine*, Vol XI (January 1901).

At first, the police force did not support this research, but later, they realized its enormous effectiveness because in 1884 it was used to identify 241 repeat offenders. In addition to his work as a police inspector, Bertillon also taught many classes explaining all his methods. Figure 2 shows two photographs of these courses.

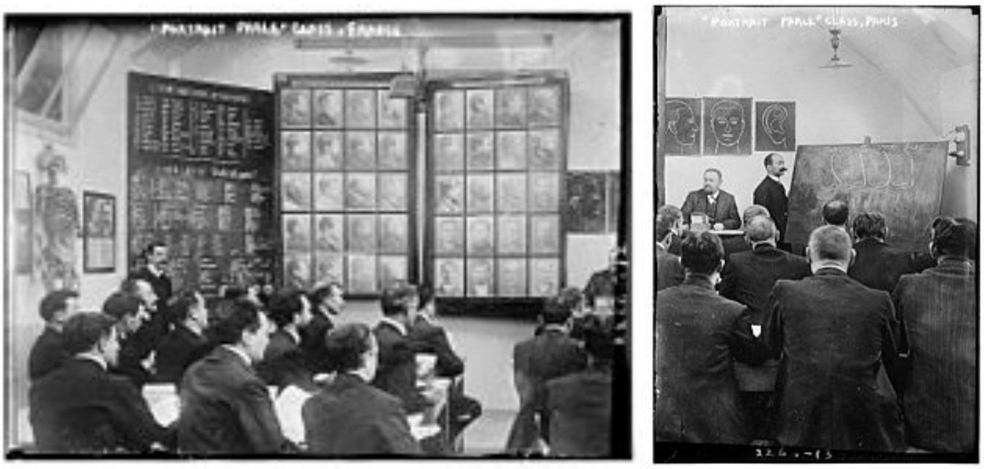


Figure 2. Photographs of classes given by Bertillon (1911).

Bertillon designed a system for identifying people based on eleven measurements of the head and body: 1) height, 2) stretched arm span, 3) seated height (from the chair to the head), 4) head length, 5) head width, 6) length of

the right ear, 7) width of the right ear, 8) length of the left foot, 9) length of the middle finger of the left hand, 10) length of the small finger of the left hand, and 11) length of the left forearm. To determine the similarity between two people, we can calculate the Euclidean distance between the vectors formed by the 11 components. If A and B are two vectors of Bertillon's 11 measurements and we want to know whether they belong to the same person, then we calculate $D_{Bertillon}(A,B) = \sqrt{\sum_{i=1}^{11}(A_i - B_i)^2}$. We consider that they belong to the same person if $D_{Bertillon}(A,B) \leq threshold_{Bertillon}$.

Figure 3 shows 9 drawings made by Bertillon himself showing how measurements should be taken. In honour of its creator, this method is called *Bertillonage*.

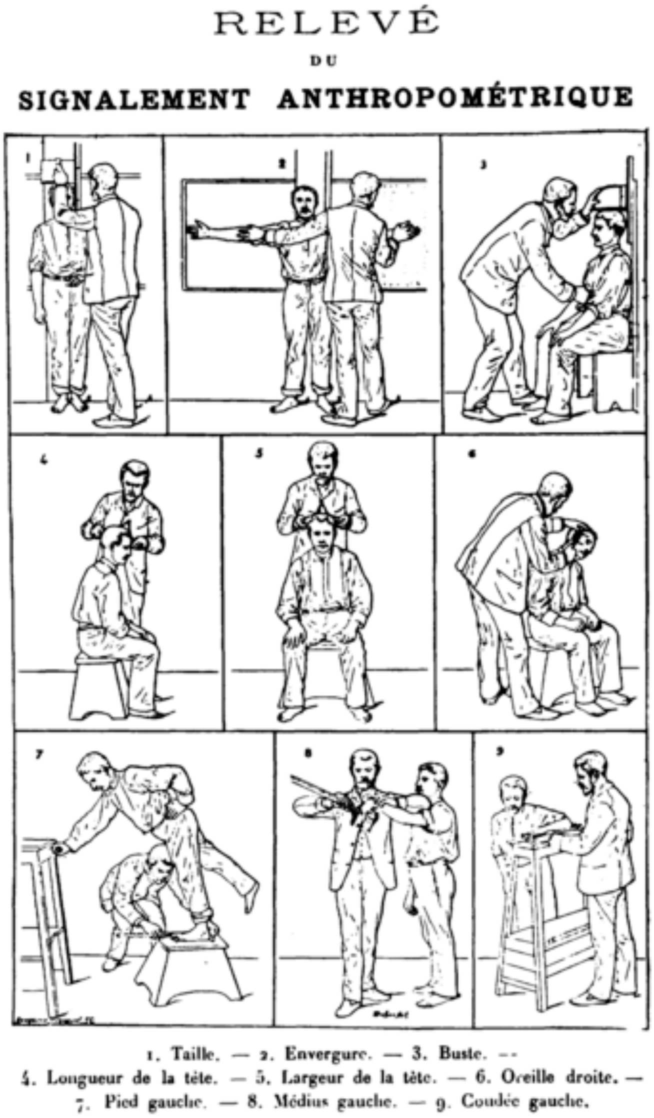
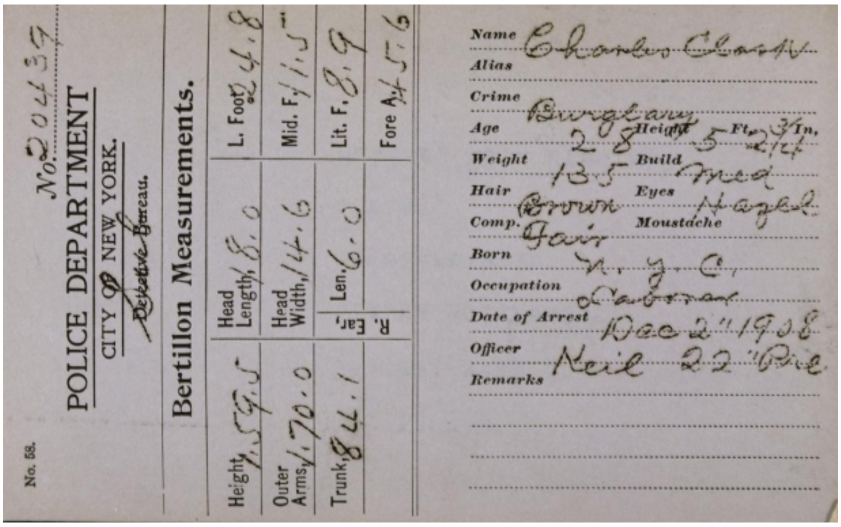


Figure 3. Image from Bertillon's book (1893) which shows the 11 measurements that were recorded in an offender's police file. Drawings 1 to 5 represent measurements 1 to 5. Drawing 6 represents measurements 6 and 7. Drawing 7 represents measurement 8. Drawing 8 represents measurements 9 and 10. Drawing 9 represents measurement 11. Figure 4 shows a file of the New York City police in which the Bertillon measurements can be seen.


POLICE DEPARTMENT
CITY OF NEW YORK.
Detective Bureau.
No. 58.
Bertillon Measurements.

Height 1.59.5	Head Length 18.0	L. Foot 24.8	
Outer Arms 1.70.0	Head Width 14.6	Mid. F. 11.5	
Trunk 84.1	R. Ear, Len. 6.0	Lit. F. 8.9	Fore A. 45.6

Name Charles Clark
Alias
Crime Burglary
Age 28 Height 5 Ft. 3 1/4 In.
Weight 135 Build Med
Hair Brown Eyes Hazel
Comp. Fair Moustache
Born N. Y. C.
Occupation Laborer
Date of Arrest Dec 2nd 1908
Officer Neil 22nd Pct.
Remarks

Figure 4. New York City Police file. Bertillon's measurements can be seen, and the date of arrest is the 2nd of December 1908.

However, Bertillon's measurements can change over time, and they are also not unique; therefore, criminal science began investigating fingerprints as this technique is considered to have a more scientific basis. Although the Bertillon method was used for years, it was severely discredited by the case of Will West and William West in 1903 (Figure 5). In 1901 William West was sentenced and imprisoned in Kansas (United States of America). As a criminal, his Bertillon measurements were taken. Two years later, in 1903, Will West was arrested and his Bertillon measurements were taken. Using this method, the police deduced that Will West had changed his name and that he was formerly called William West, that is, that he was actually William and had been previously convicted. Later, it became evident that William West was still in prison and therefore Will West was in fact another person.

Figure 5. Photographs of Will West and William West taken in prison. You can see the incredible similarity between these two people.

The Bertillon measurements of Will West were: 178.5; 187.0; 91.2; 19.7; 15.8; 14.8; 6.6; 28.2; 12.3; 9.7; 50.2. And the measurements of William West were: 177.5; 188.0; 91.3; 19.8; 15.9; 14.8; 6.5; 27.5; 12.2; 9.6; 50.3. You can see an impressive similarity in the eleven values as well as in their faces.

More than a century has passed since the head of the Buenos Aires police, Juan Vucetich (1858-1925) (Figure 6, left) discovered that Francisca Rojas had killed her two children in 1892 thanks to a bloody fingerprint (Figure 6, right) left on the mail box of her home. Initially, the servant, called Velázquez, had been wrongly condemned. This tragic event was the beginning of biometrics applied to society. A year later, in 1893, the Interior Ministry of the United Kingdom officially accepted that two people could not have exactly the same fingerprints. Therefore, many police departments saw fingerprints as a way of identifying offenders or criminals who often changed their names to avoid being given longer sentences because they were repeat offenders. Police stations began to create criminal files of fingerprints and files were created or enlarged when there were new arrests. It is important to point out that the science of biometrics based on fingerprints was found to be extremely useful in forensics and this fact brought about great scientific advances. The authorities could compare the fingerprints left at crime scenes with the fingerprints recorded at the police stations of convicted criminals who had been arrested previously, and thus identify repeat offenders.

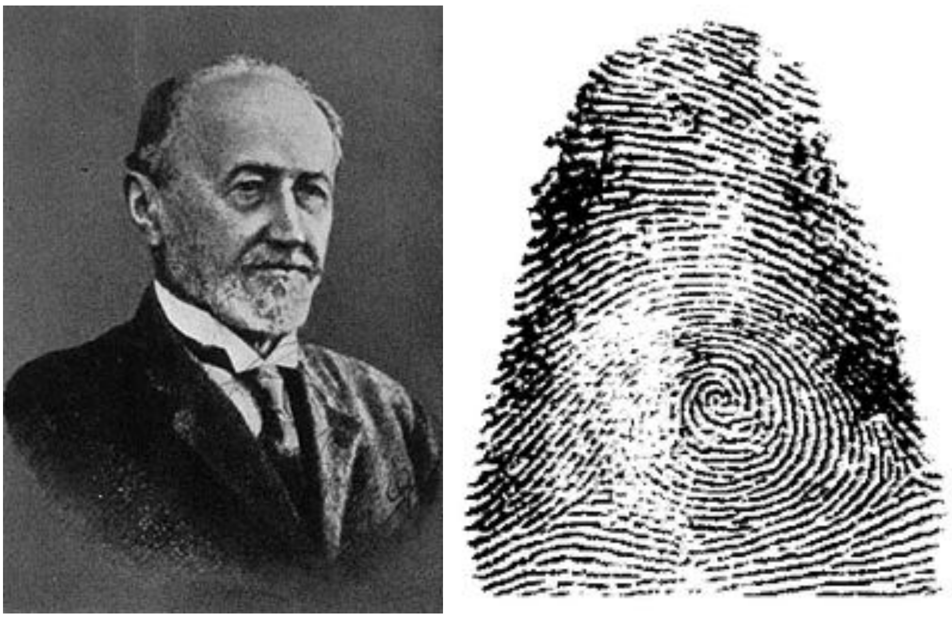


Figure 6. Photo of Juan Vucetich and the fingerprint that Francisca Rojas left on the mailbox.

The increasing number of requests for fingerprint comparisons quickly became unsustainable. Therefore, it became necessary to classify the fingerprints into a few classes (from 4 to 8 classes). When a new search was made in the files, the new fingerprints were only compared to the fingerprints that belonged to the same class. The first method for classifying fingerprints was devised by **Francis Galton** (1822-1911) (Figure 7, left) and some years later, in 1900, the Commissioner of Police of the Metropolis (London), **Edward Henry** (1850 -1931) (Figure 7, right), set up a method based on this classification in Scotland Yard.

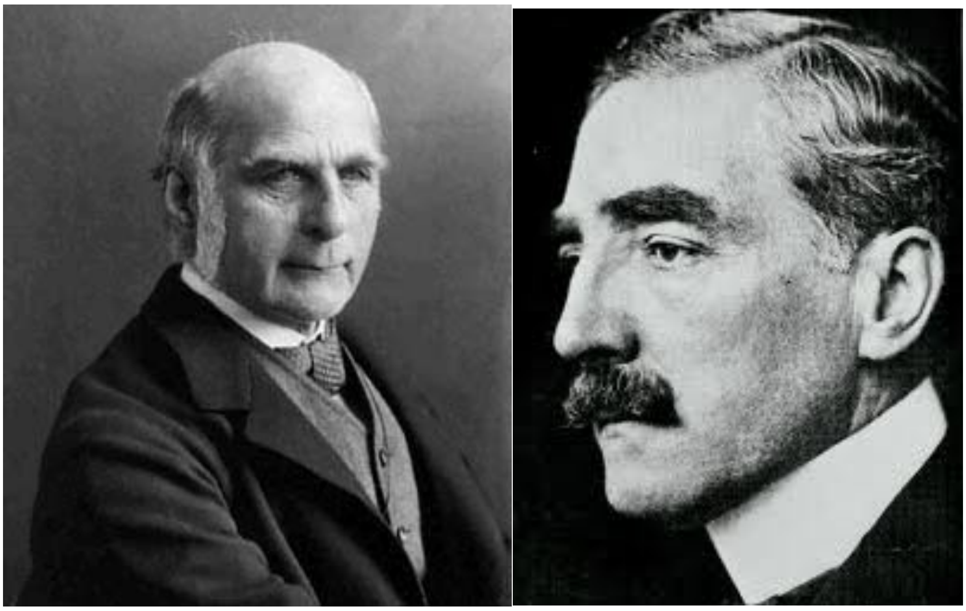


Figure 7. Photographs of Francis Galton and Sir Edward Henry

Research into methods for biometric classification and comparison (fingerprints, face, iris, hands, gait, etc.) is slow. In addition, the necessary to be extremely meticulous in searching for similarities between fingerprints, faces, irises, etc. or the class that they belong to as well as the need to visualize fingerprints in different sizes (to capture the overall information and the local details) has made it necessary to research electronic systems for acquiring and comparing fingerprints. The first efforts led to the development of the *Automatic Fingerprint Identification System* (AFIS) in the last four decades. Later, other automatic methods for faces and irises emerged. The police scientists were the first to adopt these methods.

More recently, concerns about security and identity fraud have created the need to use biometric methods in social applications other than forensic applications. We are now finding increasingly more biometric systems in everyday life, and therefore it is important that new technicians know about these technologies.

2 Biometric Recognition

We live in a digital society that is increasingly mobile. Representatives of our identity, like secret codes (common in electronic accesses) and cards (used by banks or government applications such as health cards), are not reliable for establishing a person's identity. Secret codes can often be guessed (especially if you know the person) and cards can be lost or stolen. In addition, cards and secret codes are commonly shared by friends or workmates. Therefore, secret codes and cards do not guarantee the identity of their users.

Biometric Recognition or *Biometrics* is the use of different anatomical features (fingerprints, face, iris) and behaviours (voice, signature, writing) to identify a person. These characteristics are called *biometric identifiers* or *biometric features* and serve to automatically recognize individuals. Biometrics is becoming an essential factor in the effective identification of people. This is because biometric features cannot be shared or lost and represent the intrinsic body shapes of the individual who is identified by them. Recognizing a person by their body and then linking this body with an externally established identity is a powerful tool for managing identity with enormous potential consequences, both positive and negative. Therefore, biometrics is not only a fascinating problem in the research field of pattern recognition, but also a technology, which when used correctly can make society safer, reduce fraud and provide user-friendly interfaces.

The word *Biometrics* derives from the Greek *bios* (meaning life) and *metrics* (meaning measurement). Thus, biometric features are measurements taken from the living human body. In addition, all biometric features are a combination of anatomy and behaviour. For example, fingerprints are anatomically from nature but the use of the input sensor (that is, how the user places their finger on the sensor) depends on the behaviour of the individual. It is important to mention that biometric features are often more similar in close relatives.

Every day we ask ourselves many questions related to the identity of people. Is this person authorised to enter this building? Can this person be given this information? Is this person wanted for a crime? Has this person already received some social benefits? Private companies and governments need reliable answers to these questions. Because biometric features are hard to replace, forget or share, they are considered safer for recognizing people than classic secret codes or identity cards. The objective of biometric applications is to obtain systems that are more comfortable (for taking out money from ATMs without cards), safer (only authorized people can have access) and faster (reducing the maintenance of secret codes and cards). The rise in the use of biometric technologies has led to a decrease in the price of systems, and the components have been miniaturized and are now more reliable. These factors have led to this technology being used even more.

Figure 8 shows the distribution of biometric features with respect to the income they generate. The fingerprint is the oldest biometric feature and continues to be the one that generates most economic revenues. The next biometric feature is the face, which is at a very large percentage distance. Middleware is a computer term for the entire set of applications or software routines that make up intermediate layers between biometric feature reading devices and the high-level applications used by the user.

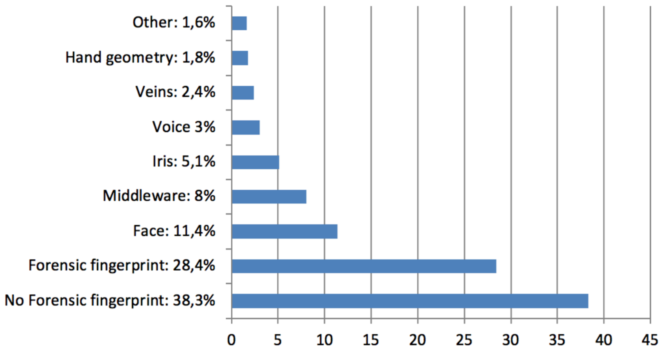


Figure 8. Percentage of income generated by the different biometric methods.

Figure 9 shows the revenue of the biometrics industry from past years and the predictions for future years in millions of dollars according to Acuity Market Intelligence ©.

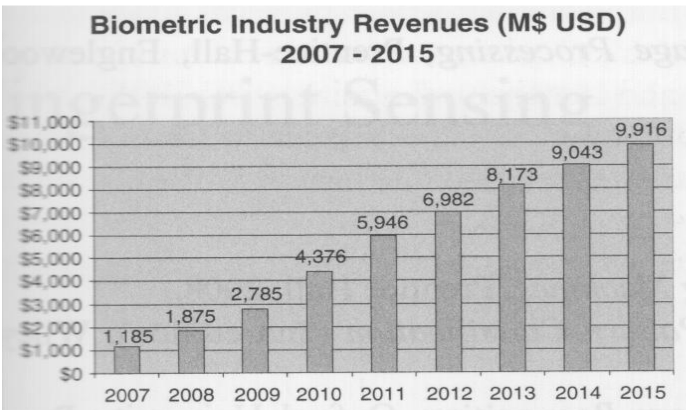


Figure 9. Income generated by biometric systems from 2007 to 2010. Revenue forecast for 2011 to 2013.

To finish this section, I'd like to comment on the reality of biometric techniques and their deployment in real applied systems. The imaginative and idealistic use of biometrics in films and television series has led to a widespread belief that biometrics is a completely discovered science and a fail-safe technology. This is not true. There are a lot of aspects that need to be researched because they need to be improved. Biometric recognition works well, there are biometric applications that work with millions of users, but research in this field still has a long way to go.

3 Biometric systems

Biometric application can be differentiated into two types of systems: *Verification Systems* and *Identification Systems*.

Verification systems (also called *authentication systems*) authenticate the identification of the person by comparing the recently captured biometric feature with the biometric feature that has been previously captured by the system in the enrolment process. The user must present their identification by means of a card or secret code. The system carries out a single comparison between the biometric feature that the user has just presented and the biometric feature in the database that matches the identification presented by the user. The output of a verification system is usually binary: it is the same person if the biometric features match (they are very similar) or it is not the same person. In some cases, the biometric features and the identification in the database are encrypted in the user's card. In this case, we have a database distributed among all the users' cards.

Identification systems recognize the person by searching in a database for the biometric feature that most resembles the feature used to identify the person. Unlike in verification systems, the user does not provide any information about their identification. The system makes a comparison of one to many. This means that the biometric feature of the unknown user is compared to many biometric features in a database. This system can have several outputs. The simplest output is to return the name of the person (identifier) whose biometric feature is similar to the one introduced. Another possibility is to deduce that this biometric feature does not belong to any person in the database (this occurs when the distance between the biometric feature and all the biometric features in the database is greater than a certain threshold). Finally, and this is the most common case in forensic applications, the system does not return a single person but rather a *list of candidates*. That is, it returns people for whom the distance between their biometric features and the biometric feature that has been introduced in the system is less than a certain threshold.

Both the verification and identification systems require a prior process called *Enrolment*. This process is responsible for collecting a person’s biometric feature (or biometric features) together with their identification. This process is very important because it is responsible for relating (for life!) the person’s identification with the specific biometric features. Normally, this process is carried out in front of an authorized person who oversees the authenticity of the data provided by the user (identity card, passport, etc.) and makes sure that it is really this user who provides the biometric feature to the system. In addition, this person verifies the quality of the biometric data obtained during the enrolment process. If they believe that the data do not have sufficient quality, they ask the user to present the biometric feature (fingerprint, face, iris, etc.) to the system again. It is essential that the data that are stored in the database are of the highest quality, since in the identification and verification processes this quality cannot always be guaranteed. Some systems require the user to capture the same biometric feature several times (usually 3 times). The system can choose the best image or merge them and thus reduce capture errors.

The three systems mentioned above use the following processes (Figure 10):

- *Capture*: The digital representation of the biometric feature must be captured. The biometric sensor is usually a system for capturing an image (except when a speaker is identified, then the sensor is a voice recorder). Normally, the captured information is called a *Sample*. Sometimes, the capture system also includes other peripherals to introduce non-biometric information or display information.

- *Feature Extraction*: With the aim of facilitating comparisons, increasing information and reducing noise, the original digital representation (digital image) is normally processed by a feature extractor to generate a more compact and identifying representation called the *identification register* or *feature set*.

- *Template Creation*: The *template* is a compact way of representing a set of samples of a single biometric feature (for example, you can create a template of 16 different samples of the image of one person's face). The template creation process receives the identification records as input and creates more-compact information with the aim of extracting the information that persists in all the samples. This persistent information is considered the characteristic features. In some cases, this template is made up of only one sample and can therefore be represented as an identification record.

- *Comparison*: The comparison process receives an identification record and a template as input and calculates a distance between the two. Sometimes, instead of a distance, it obtains a probability that they represent the same individual. In the verification process, there is an internal threshold in the system that can only be modified by the system administrator. If the distance is less than the threshold (or the probability is greater than the threshold), the system considers that the two pieces of information come from the same person, otherwise, it considers that they come from two different people.

- *Selection or Filtering*: In identification systems with a lot of data (we are talking about 50 million fingerprints), filtering is a method for increasing the system's response time. Typical database techniques make it unnecessary to explore the entire database and thus time is gained.

- *Data Storage*: This is the process for storing the user information. This information is composed of a unique identifier (for example, the national identification number or passport), the biometric template and other data (for example, address, profession, etc.). Depending on the application, the data is stored in centralised storage systems (used for identification) or *smart cards* (used for verification). In addition, encryption techniques are applied with all the data so that the registration format of the identification number and the biometric features are indivisible.

Depending on the application domain, a biometric system can operate as an *online* system or an *offline* system. *Online* systems require that the comparison is carried out quickly and that there is an immediate response. For example, permission to start an application, or a person's physical entry into a facility. They are usually verification systems. *Offline systems* do not require the response to be immediate and an admissible delay in the response is tolerated. These are usually identification systems. *Online* systems are usually completely automatic and require the biometric feature to be captured with an electronic sensor and there is no human control of the data quality. On the other hand, *offline* systems are usually semi-automatic. The biometric feature can be captured with a non-electronic system (for example, capturing a fingerprint left at the crime scene) and a specialist supervises the data quality. In addition, this specialist has computer tools to fix the data or help the program that performs the biometric comparison.

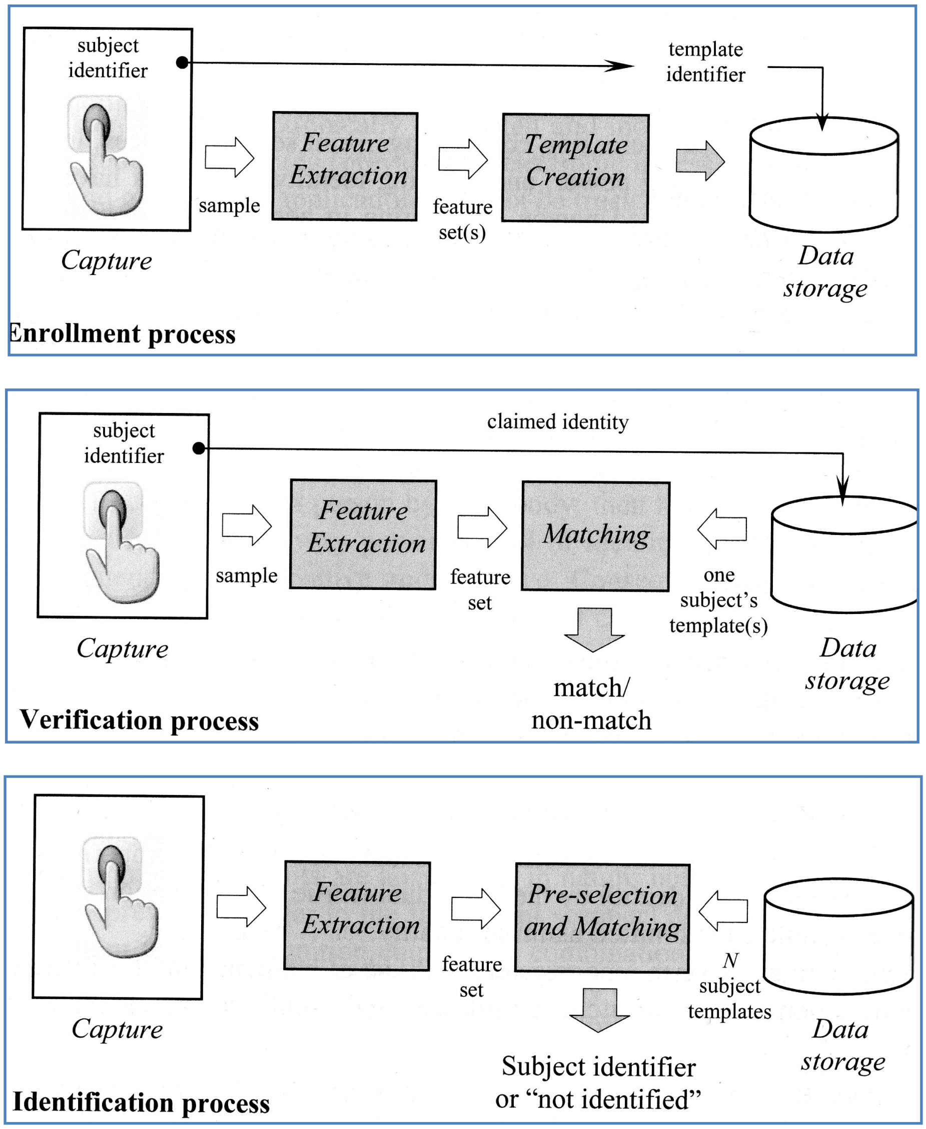


Figure 10. Stages and processes that make up the systems of (a) enrolment (b) verification and (c) identification.

Depending on the application, two types of searches are carried out in identification systems. *Positive searches* and *negative searches*. The first ones are those in which we want to verify whether the biometric feature is in the database, that is, whether the user has been enrolled. We wish to know the identification of that biometric feature. The most usual case is to introduce a fingerprint that we have found at a crime scene, or a face that we have been able to photograph, into the system to determine who it belongs to. On the other hand, *negative searches* are those in which we want to verify that the individual has not been enrolled before. We want to know that no person has enrolled with these biometric features. The most usual application of this is for making sure that a person does not use a service more times than they are authorised to do. For example, that they do not collect a state aid several times or do not vote several times in an election.

4 Biometric features

Any anatomical trait or human behaviour can be used as a biometric identifier to identify or verify people if it fulfils the following requirements:

- **Universality**: Everyone must possess this biometric feature.
- **Particularity**: Everyone must be sufficiently different in terms of the biometric feature.
- **Permanence**: The biometric feature should not change over time or due to any other factor from the point of view of comparing biometric features.
- **Measurable**: The biometric feature must be able to be measured quantitatively.
- **Performance**: The biometric feature must guarantee precision and robustness in different environmental factors.
- **Acceptability**: Users of the system must accept the use of this biometric feature for identification.
- **Unfalsifiable**: The biometric feature must be difficult to falsify. (This is the main theme of Module 6).

A biometric system must have acceptable accuracy and speed with a reasonable number of resources. In addition, it cannot be harmful to users, it must be accepted by potential users and sufficiently robust to fraudulent methods.

A fairly large number of biometric features are being used in different applications. This is because each biometric feature has its own strengths as well as weaknesses and it is necessary to use a specific number of resources. The biometric features must be able to adapt to the specific application for which the system has been designed. Which feature can be used in a given application is decided considering the characteristics of the application as well as the properties of the biometric feature. The main issues that must be considered when a biometric feature is selected for a specific application are:

- Does the application need a verification or identification system? If the application requires the identification of a person in a very large database, then it needs a biometric feature with a lot of particularity.
- What are the operational characteristics of the application? That is, will it be used in a semi-automatic or completely automatic system? Indoors or outdoors?
- Are users accustomed to showing or agree to showing this biometric feature?
- What is the storage capacity of the application? For example, an application that works with a smart card has very limited storage resources.
- Is it very important that the biometric feature cannot be falsified?

Next, we discuss the most common biometric features that have been used in commercial systems and which are currently being researched.

Head biometric features:

- **Face**: The face is one of the most acceptable biometric features because it is the most common biometric feature used by humans for recognizing people as well as daily visual interactions. In addition, the method for acquiring images of the face is nonintrusive and there is no need for user interaction. In the prototype phase, we find some methods that not only recognize the person but also their mood according

to their facial expression, age, sex and position. Some cameras already include a smile detector, which not only detects faces, but also detects whether they are smiling.

- **Facial thermogram**: This technology can be used along with face recognition in passive tracking (the user does not know that they are being identified). It has the advantage of not being affected by people wearing make-up or by their haircut or facial hair. However, it has the disadvantage of being affected by a simple cold or by the person doing sport. It works with a thermal camera at a maximum distance of a few meters.
- **Ear**: The ear shape is a very useful biometric trait for passive recognition of a person. A security camera can easily film an ear. This biometric feature remains fairly stable over time; however, a person's ears are often hidden by hair or a hat. To obtain similar operating characteristics, it is usually used as a complement to face or gait (way of walking) recognition.
- **Iris**: The visual texture of the human iris is determined by the chaotic process and genetic morph during embryonic development. It has been suggested that it is different for every person and each eye. An iris image is usually captured using a contactless capture process. Normally, capturing an image of the iris involves the user's cooperation, although there are systems (in the laboratory prototype stage) for capturing an image of the iris without the user's cooperation. The user collaborates in placing the image at the centre of the capture device and ensures that the iris is at a predetermined distance in the focal plane of the camera. Iris technology has proven to be very accurate and fast when the image has a high resolution and has been captured well.
- **Retina**: This biometric feature is one of the latest to be incorporated. Its technology and application are very similar to those of the iris and has been shown to be highly discriminatory. It is based on reading the small veins in the retina, which is the membrane inside the eye that captures light when we are seeing. The image is captured with infrared light and therefore this technology is of low acceptance.

Hand and finger biometric features:

- **Geometry of the hand and fingers**: The length and width of the fingers, as well as the relationship with the hand width are biometric features that do not change very much, although they are not very distinctive. The system for acquiring the hand and finger geometry needs user collaboration to capture the front and side images (some systems only use the front image). The storage requirements of this technology are very small, which makes it very attractive for systems with limited memory. However, due to the limited ability to distinguish different users, it is only used in verification processes and is not suitable for identification applications.
- **Fingerprint**: The fingerprint is the pattern of ridges and valleys on the fingertip that is formed during the first months of pregnancy. It has been determined empirically that the fingerprints of twins and the fingerprints from different fingers of one person are different. In addition, for over a century it has been proven to be a technology that is highly discriminatory even in databases with over 50 million users. Today, fingerprint recognition is a technology that is very easy to install and inexpensive. A finger scanner bought on a large-scale costs about 50 euros. Finally, it is a technology that is useful in forensic applications and maximum security applications. In addition, there is only a very small fraction of the population that cannot use this technology.
- **Hand print**: Human palms contain ridges and valleys like the fingers. The palm has more area and therefore it is expected to be more discriminating than fingerprints. However, hand scanners are large and expensive, and therefore cannot be used in some applications where devices need to be small. The

advantage is that the palm contains lines that are more marked and can be captured with low resolution devices (cheaper).

- **Hand and finger veins**: The structure of the veins of the hands and fingers is detected with near-infrared light from a hand pressed down on the capture system (infrared scanner). This system is currently marketed as the infrared scanner uses LED diodes, which are economically affordable.

Body biometric features:

- **Smell**: Everyone exudes an odour that is characteristic of their chemical composition and can thus be used to identify individuals. The most common system is composed of an array of sensors where each sensor detects a specific type of chemical (or aromatic component). The system response consists in the amount of the aromatic component detected by each sensor. After smelling, the system must be initialized with completely clean air. The technology for automatic identification of odours (in any application, not only biometric identification) is being researched and currently there are few real systems (that are not laboratory prototypes) in operation and none for identifying people.
- **DNA**: Deoxyribonucleic acid is the one-dimensional code that characterises the individual *par excellence*, except that identical twins have the same DNA. It is usually used for identifying people in forensic applications; however, it cannot be used in real-time applications because it needs a few hours in a laboratory to isolate the DNA correctly and extract the basic information. In addition, the use of information from DNA tends to worry people because it can also give information that a person is suffering from certain diseases or is likely to suffer from them.

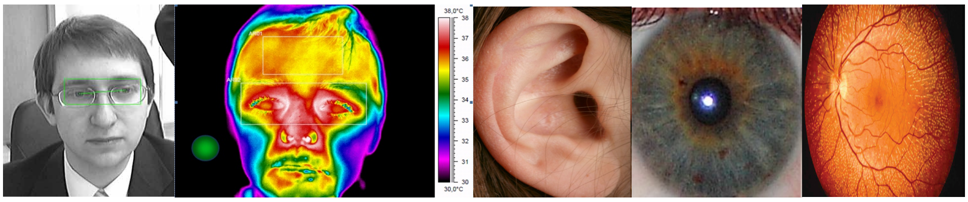
Behavioural biometric features:

- **Speech**: Speech recognition is the system that is least intrusive as users do not need to have an image taken. Moreover, it is a system that can be used through a phone without an image. However, the voice is not sufficiently distinctive to allow identification in a large database. In addition, the voice degrades easily depending on the microphone, communication line or scanning systems. It is also important to consider that the voice can be changed greatly by the user's health (sore throat, cold, stress, strong emotions, etc.). In addition, some people seem to be very good at imitating the voices of others; therefore, there are potential fraudulent users.
- **Signature**: Signatures have been accepted in commercial, legal and government transactions for centuries. The way people write their name is a behavioural biometric characteristic. However, it is important to consider that some people's signatures vary greatly over time, conditioned by physical and emotional conditions. In addition, professional falsifiers can reproduce signatures so they look identical to the naked eye.
- **Gait** (way of walking): This refers to the biometric feature of the way a person usually walks: the pace and speed of your moving legs, whether you have a long step, whether you swing a lot. It has the advantage that it is one of the few biometric features that can (and in fact must) be measured at a distance, which makes it well suited for applications for monitoring and identifying people. Most algorithms extract the silhouette of the person to identify and deduce the spatio-temporal attributes of their movements. This biometric trait has the disadvantage that it is not very permanent because not only does it vary with time but it is affected if the person is carrying heavy bags, if the person is tired and also by the clothes they are wearing.

- **Way of typing**: Everyone has their own specific and repetitive way of typing when they use a sequence of keys. This biometric trait cannot be used to identify a person but it can be used to verify whether a person is the one who is currently typing (or there is a probability that it is). Usually, this is a biometric feature that is used in a concealed way through a program installed in the computer that the person is typing on. It makes it possible to verify that the person typing has not changed during the work session because it is a biometric characteristic that can be verified continuously.

Figure 11 shows images of the biometric traits outlined above.

Head biometric features:

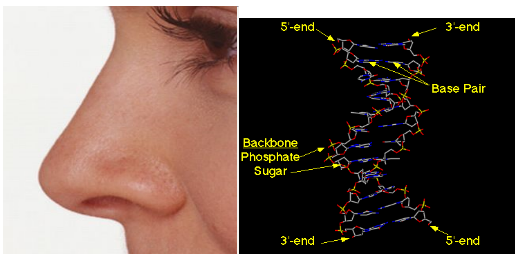


a) b) c) d) e)

Hand and finger biometric features:

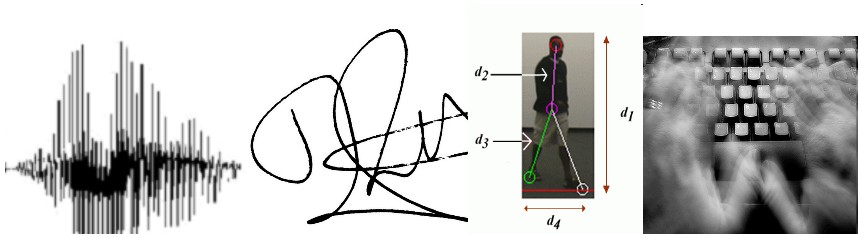
f) g) h) i)

Body biometric features:



j) k)

Behavioural biometric features:



l) m) n) o)

Figure 11. Images of the main biometric features distributed according to their location and whether they are physical or behavioural. a) Face b) Facial thermogram c) Ear d) Iris e) Retina f) Hand geometry g) Fingerprint h) Hand print i) Veins of the hand and fingers j) Smell k) DNA l) Speech m) Signature n) Gait o) Way of typing.

The following tables (Table 1 - Table 4) show the main characteristics that a biometric system must have for the various biometric features. The table entries show the goodness of each characteristic in each biometric feature separated into three values: H(high), M(middle) and L(low).

Biometric feature	Universality	Particularity	Permanence	Measurable	Performance	Acceptability	Unfalsifiable
Face	H	L	M	H	L	H	H
Facial Thermogram	H	H	L	H	M	H	H
Ear	M	M	H	M	M	H	M
Iris	H	H	H	M	H	L	H
Retina	H	H	M	L	H	L	H

Table 1. Goodness of head biometric features.

Biometric feature	Universality	Particularity	Permanence	Measurable	Performance	Acceptability	Unfalsifiable
Fingerprint	M	H	H	M	H	M	M
Hand print	M	H	H	L	H	M	M
Hand geometry	M	M	M	H	M	M	M
Hand veins	M	M	M	M	M	M	H

Table 2. Goodness of hand and finger biometric features.

Biometric feature	Universality	Particularity	Permanence	Measurable	Performance	Acceptability	Unfalsifiable
Smell	H	M	H	L	L	M	L
DNA	H	H	H	L	H	L	H

Table 3. Goodness of body biometric features.

Biometric feature	Universality	Particularity	Permanence	Measurable	Performance	Acceptability	Unfalsifiable
Signature	L	L	L	H	L	H	L
Gait	M	L	L	H	L	H	M
Way of typing	L	L	L	M	L	M	M
Speech	M	L	L	M	L	H	L

Table 4. Goodness of behavioural biometric traits.

The fingerprint has a great balance between all the features. Almost everyone has fingers (except for people with hand disabilities). History has shown that fingerprints are distinctive and permanent even if they are cut or burnt. In addition, current sensors capture fingerprints at very high resolution at an affordable price and do not have the problem of needing to differentiate the fingerprint from the background like faces. The main inconvenience is that you cannot capture fingerprints at a distance and without the knowledge of the person as you can do with their faces. Finally, fingerprints and the templates they generate are becoming increasingly difficult to falsify thanks to life detectors (that detect blood flow or oxygen in the blood) and encryption techniques.

Another characteristic feature that has a high performance, in relation to the biometric characteristics, is the iris. It has been proven to have high universality, particularity and permanence. Its two weak points are its low social acceptance (related to the difficulty of capturing an image of the iris) and the fact that it is not useful for search applications in forensic tests like fingerprints that are left at crime scenes. However, it is beginning to prevail because it has shown to be more particular than fingerprints.

It is interesting to also consider hand geometry. Despite only having "measurable" as a high-quality characteristic, it is useful in some low security applications due to its speed, low cost and because it is so easy to measure.

Finally, there are some biometric features that are not very measurable. This clearly shows that they are not useful in some applications where speed and simplicity of the system are essential. The most extreme case is DNA, which needs hours in a laboratory to make a comparison.

5 Applications of Biometric Systems

Biometric systems are deployed in a variety of different application environments. Applications range from forensic checks and controls for electoral systems to mobile phones. However, the design and tuning of the systems depend on the context and categories of the applications that in turn define the requirements of the application.

5.1 Application Context

The applications can be categorised according to the following contexts:

- **Cooperative versus non-cooperative**: In a cooperative system the user must interact or cooperate with the system to be recognized, for example, by focussing their iris in the middle of the image. An example of the non-cooperative system is a face identifier when you walk through a door without the system requiring that you stay still or look at the camera.
- **Habitual versus non-habitual**: habitual systems are those in which the users access the system on a regular basis, that is, each day when they arrive at work or a businessperson who goes through airport checks once a week. An example of a non-habitual system is the one that requires a fingerprint to renew a driving license every five or 10 years. It is an important factor in the system's design because it has been proven that if the user is used to interacting with the system, this greatly increases the accuracy of the system.
- **Supervised versus unsupervised**: Supervised systems are those that the process of acquiring the data is supervised, observed and guided by a person (e.g. a manager or security officer). Within supervised systems we can distinguish those that the supervision is only carried out at enrolment (for example, an ATM with a biometric system) or that supervision is carried out in the enrolment and verification (airport checks).
- **Standard operating environment versus non-standard**: Standard operating environments are those that people are used to in terms of light, humidity, noise, etc. Normally, the systems that operate in closed environments (computer access) are considered standard systems. So are the systems in open environments but under normal conditions. External systems can be considered non-standard if the conditions are special (very low temperatures, snow, strong wind, etc.).
- **Private vs. Public**: Users of private systems are direct customers or employees of an organisation that has developed and deployed a biometric system. These users are specifically classified because they are users who are used to using these biometric systems and believe in biometrics. These users are potentially very good at facilitating the process of enrolment, verification or identification and therefore the percentage of error generated is usually very low. Public systems are the rest of the systems.
- **Open versus closed**: In open systems, the user template stored in the database can be used in various applications. For example, the user can use their fingerprint to access their computer or their electronic banking system. In open systems, there is a single enrolment and a single database. In closed systems, the user must make two enrolments and there are two databases. In open systems we need to use standard formats and currently this is not usual because most organisations use their own format.
- **Declared versus undeclared**: Declared systems are those that the user knows about and accepts the interaction with the biometric system. The user knows they are presenting their iris, face or fingerprint to the system to be recognized. In undeclared systems, the user does not know that a biometric system

is being applied to identify them. An example would be a system in waiting rooms or airport corridors. While you are quietly reading or walking, there could be hidden cameras used to detect people who are wanted for breaking the law.

5.2 Application categories

There are two ways of categorising the applications, *horizontal categorisation* and *vertical categorisation*. In horizontal categorisation the categories are applications that have a common purpose or environment. In vertical categorisation the categories are based on the needs of each sector of the industry or government. Below is a list of application types according to the categories.

Horizontal categories

- **Physical access control**: Biometrics serve to restrict access in facilities like nuclear power plants, military areas or safe deposit boxes in banks. As well as in not-so-high security areas such as private clubs, museums or public pools.
- **Logical access control**: Access to remote desktops or servers and database. Increasingly, this is for computer programs that can only be used by authorized people. For example, in computer programs used by hospitals, doctors are authorized to modify the data, but nurses are only authorized to view the data but not change them.
- **Authentication of the user in transactions**: Financial transactions can be ordered from ATMs or PCs from remote locations. Biometrics adds security to the transaction to reduce fraud and because the person who orders the transaction does not deny having ordered it later.
- **Access Control Devices**: Personal electronic devices such as laptops or mobile phones often contain personal or confidential data. These data are usually protected by a PIN number, but they are increasingly being protected with a biometric feature (currently, the most widely used is the fingerprint or face).
- **Time and presence**: Applications called *time and presence* are those that monitor the location of employees or company vehicles at all times and are also used to pay salaries according to these parameters. Adding a biometric control ensures that it was really that specific worker who has been in a particular location.
- **Civil identification**: One of the most important objectives in civil identification applications is to prevent multiple enrolments and find duplicates. For example, copies of passports, driving licenses, national identity documents. It is also an objective to discover whether a person who is wanted by the police is enrolled. The introduction of biometric features in these applications is a crucial factor.
- **Forensic identification**: Comparing fingerprints left at a crime scene with those in a criminal database is the oldest application of biometrics. Currently, faces, ears, and gait filmed by security cameras are also being included. Latent ear prints (of a person who leans against a door to listen to what is being said on the other side) or marks of the whole hand are also looked for.

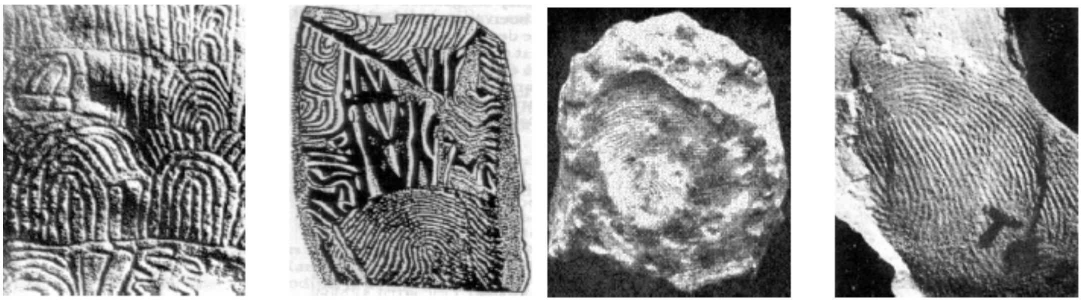
Vertical categories

- Health: hospitals, primary medical care, ambulances.
- Finance: financial transactions.
- Receptions: casinos, hotels, public pools.

- Sales: department stores, petrol stations.
- Education: control access to schools, university dining halls.
- Manufacturing: monitoring workers.
- Technology: mobile devices, telecommunications.
- Transport: monitoring passengers, buying tickets.
- Public Institutions: state, municipalities, department of justice.
- Military: control access to restricted areas.

6 History of Biometrics

A few historical objects have been discovered on which it could be "inferred" that there are fingerprints or palm prints. For example, it seems to be possible to perceive fingerprints on Neolithic sculptures from the island of Gavrinis dated from the year 3500 BC (Figure 12.a). It is also possible to deduce marks on the famous stones dated 2000 years before Christ from Goat Island (Figure 12.b). It is important to emphasise that it has not been possible to demonstrate that these objects really show fingerprints or palm prints or that there is an express desire on the part of the possible author that these marks actually represent biometric features. However, it seems that there is sufficient scientific evidence that there really is a desire to identify the person who supplied the object through marks found on a Chinese clay stamp dated 300 BC (Figure 12.c) and on a lamp of Palestinian origin dated from 400 AD (Figure 12.d).



(a) (b) (c) (d)

Figure 12. Images of objects on which the presence of biometric features can be inferred. The two on the left are unlikely and the two on the right are more probable. From left to right: a) Neolithic sculpture on the island of Gavrinis (Year 3500 BC), b) Rocks on Goat Island (2000 BC), c) Chinese clay seal (300 BC) and d) Palestinian lamp (400 AD).

Forerunners to biometrics were the pseudo-sciences called *Phrenology* and *Anthropometry,* which served to facilitate the beginnings of biometrics.

Phrenology studied the structure of the skull to determine people's character and mental capacity. It was founded by the German **Franz Joseph Gall** (1758-1828) (Figure 13, left) at the beginning of the nineteenth century in Germany. Gall believed that certain mental characteristics could be related to certain forms and characteristics of the skull. This concept was developed further by the Italian **Cesare Lombroso** (1835-1909) (Figure 13, right) who united the concepts of Phrenology with criminal behaviours. These beliefs were most influential in the USA until the end of the 19th century.

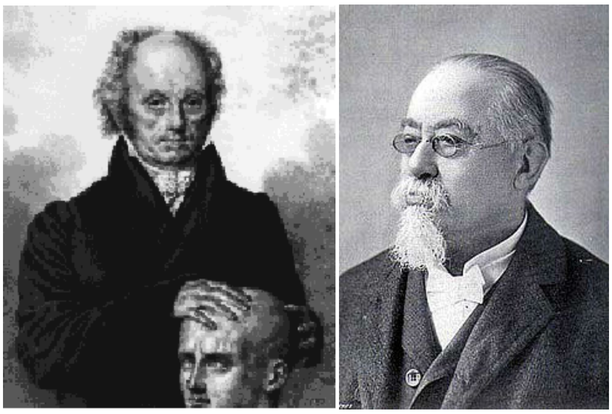


Figure 13. Portraits of Franz Joseph Gall and Cesare Lombroso.

Anthropometry was created by Belgian **Adophe Quetelet** (1796-1874) (Figure 14) in 1871. It is based on studying the measurements of the human body for classification and comparison. In 1871 Quetelet published the thesis “L’anthropométrie ou mesure des différents facultés de l’homme”. In addition to being used to create files of biometric features in police stations or prisons, it was used to classify potential criminals based on their facial features. For example, Cesare Lombroso, in the document entitled "Criminal Anthropology" published in 1895, stated that criminals have prominent jaws and that pickpockets have long hands and thin beards. This part of Anthropometry was quickly considered to be unscientific. However, the identification of criminals with the characteristic features discussed in the introduction of the module, called Bertillonage, was used in France during the first half of the 20th century. As already mentioned, it was discarded due to its low particularity and to give way to the technology of fingerprints.

Figure 14. Portrait of Adophe Quetelet.

At the same time that Phrenology and Anthropometry developed, interest in fingerprints and hand geometry began to grow. In 1823 the Czech **Jan Evangelista Purkinje** (1787-1869) (Figure 15), while studying the sweat glands, realized that the crests and valleys that we have on the skin of our fingertips always create different drawings. This was the first time that this fact was mentioned; however, at no time did he suggest that these characteristics could be used for identifying people.

In the late nineteenth century, the Scotland Yard police launched a system to classify and identify people by their fingerprints. The person in charge was the Police Commissioner called **Edward Henry** (1850-1931) (Figure 7, right). This system was based on a scientific methodology to classify fingerprints into a few classes (maximum of 6) developed by the Englishman **Francis Galton** (1822-1911) (Figure 7, left) in 1892. The system was called *Galton-Henry*. The number of followers of the Bertillon method gradually decreased while the followers of the Galton-Henry method began to increase.

Figure 15. Portrait of Jan Evangelista Purkinje.

7 Biometrics, Cinema and Art

This section discusses the influence of biometric advances on cinema. We also discuss how biometrics was used to determine the authorship of a work of art that until now was considered to be by an unknown author.

7.1 The Cinema of Biometry

Cinema has always evolved along with science, sometimes advancing and predicting, at other times inventing, and at other times simply showing reality. In 1951, we find ourselves with the movie, *Fingerprints don't lie* directed by Sam Newfield (Figure 16, left). In this film, fingerprints were not only in the title but were also the main plot of the film. Despite seeming to be an irrefutable test, the fingerprints turn out to be false and the policeman, who knows how to falsify them, demonstrates that he is the murderer.

A few years later, science continues to evolve and so does cinema. In 1968, Stanley Kubrick directed one of the most influential science fiction films, *2001: A Space Odyssey* (Figure 16, right). The spacecraft computer, called HAL, is able to see people's faces and deduce what they are saying just by reading their lips. Kubrick, in 1968, thought that in 2001 a machine would be able to read people's lips. Today, we still haven't managed it.

Figure 16. Poster of the movie *Fingerprints don't lie* and a frame of the movie *2001: A Space Odyssey*.

In 1971 the film *Diamonds Are Forever* appeared, directed by Guy Hamilton. Tiffany Case finds a fingerprint on a drinking glass. They photograph it and scan it and discover that James Bone is actually Peter Franks. But Q pretends to be James Bone with a false finger (Figure 17) .

Figure 17. Photo frames of the movie *Diamonds Are Forever*.

And now in the 80s, iris recognizers appear in the cinema. Two examples are *Blade Runner*, 1982 (Figure 18), directed by Ridley Scott, in which an iris study is used to identify whether the "person" has been created in a factory.

Figure 18. Photogram of the film *Blade Runner*.

And the classic science fiction film, *Star Trek II: The Wrath of Khan*, 1982, directed by Nicholas Meyer (Figure 19), in which people are identified by their retina.

Figure 19. Photograms of the movie *Star Trek II: The Wrath of Khan*.

In 1997, *Alien: Resurrection* by Jean-Pierre Jeunet was released (Figure 20, left). In it a computer asks the spaceship's commander to identify themselves, the commander breathes into the machine, it answers that that is the correct identification and opens a security door. In a later scene, a girl tries to open the same door, and when the machine asks her to identify herself, the girl takes out a bunch of bottles with liquid inside (like a thief who carries a bunch of skeleton keys), she sprays the sensor, the machine answers that the identification is incorrect, she tries again with another bottle and the machine greets her with the commander's name and opens the door.

In *Gattaca*, 1997, directed by Andrew Niccol (Figure 20 right), which by the way is formed by the initials of the components of DNA, adenine (A), guanine (G), thymine (T) and Cytosine (C), DNA is identified to find out whether people are free from diseases. This movie is interesting from the ethical point of view since it shows biometrics used for selecting people.

Figure 20. Photogram of the movie *Alien: Resurrection* and poster of the movie *Gattaca*.

And now in the current millennium, in *Mission: Impossible II*, 2000, directed by John Woo (Figure 21), they use a retina identifier to read the mission, a facial recognizer to identify John McCloy and a speech recognizer is falsified using a recording.

Figure 21. Photograms of the movie *Mission: Impossible II*.

In the movie, *Minority Report*, 2002 directed by Steven Spielberg (Figure 22), people are identified through their iris to make customized advertising. This is another example of intrusion.

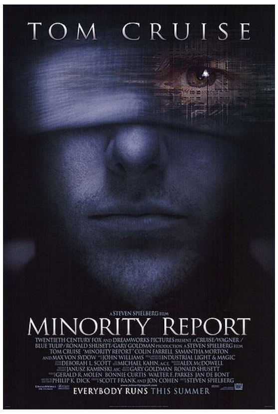


Figure 22. Photograms of the movie *Minority Report*.

And another good classic, *I, robot*, 2004, directed by Alex Proyas (Figure 23), shows us access control based on the side of the fist and a speech identifier to access files.

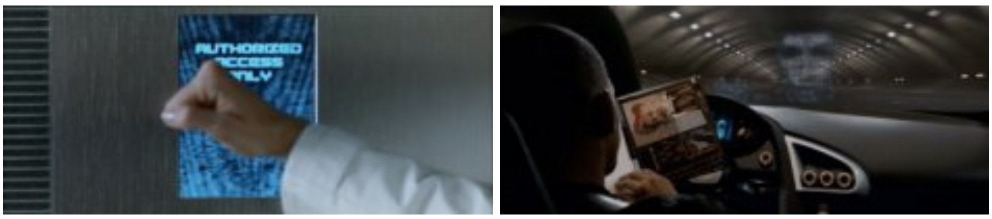


Figure 23. Photograms of the movie *I, robot*.

And finally, in 2009, there is the book *Angels & Demons*, written by Dan Brown (Figure 24), and taken to the screen by Ron Howard. In this case, the baddie manages to take the antimatter by taking out the eye of the scientist who has it. If they had installed an iris sensor with a life detector this would not have happened.

Figure 24. Photograms of the movie *Angels & Demons*.

Table 5 is a summary of the films and the biometric feature used. As you can see, there is a large variety.

Year	**Title**	**Director**	**Biometrics**
1951	*Fingerprints don't lie*	Sam Newfield	Fingerprint
1968	*A Space Odyssey*	Stanley Kubrick	Speech
1971	*Diamonds Are Forever*	Guy Hamilton	Fingerprint
1982	*Blade Runner*	Ridley Scott	Iris
1982	*Star Trek II: The Wrath of Khan*	Nicholas Meyer	Retina
1997	*Alien: Resurrection*	Jean-Pierre Jeunet	Breath
1997	*Gattaca*	Andrew Niccol	DNA
2002	*Minority Report*	Steven Spielberg	Iris
2000	*Mission: Impossible II*	John Woo	Retina
2004	*I, robot*	Alex Proyas	Side of fist Speech
2009	*Angels & Demons*	Ron Howard	Iris

Table 5. Films and the biometric feature they deal with.

7.2 Biometrics and Art

Figure 25 shows an image of a painting that until now was considered to be by an unknown author. It is known as "*The Beautiful Princess*". In 2007, it was sold for $19,000 to a New York art gallery by an anonymous Swiss collector. However, now it is considered that it was painted by Leonardo da Vinci and has been priced above 150 million dollars. This is because a fingerprint of this artist has been found on the painting. This fingerprint can be seen inside the rectangle and it is enlarged in the image on the right.

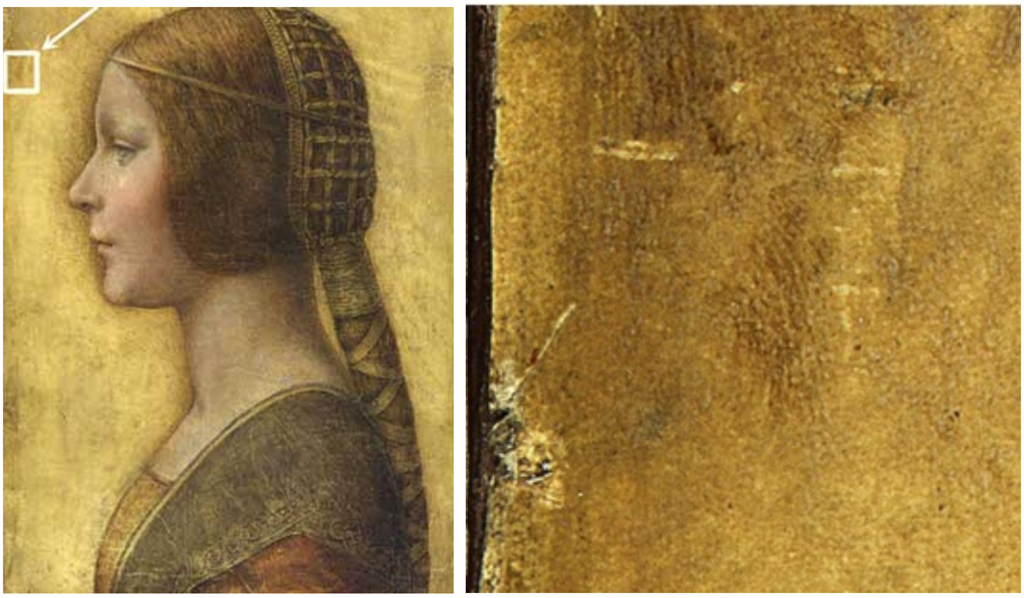


Figure 25. Reproduction of the painting "*The Beautiful Princess*" and a detail of the fingerprint that could be from Leonardo Da Vinci.

8 Reflections on a Biometric Society

This section has been taken in part from the publication in the newspaper AVUI on 3 July 2010 (http://www.elpuntavui.cat/noticia/article/7-vista/8-articles/189842-una-societat-biometrica.html).

In Spain there is no specific law to regulate the use of biometrics. The closest regulations are those of the personal data protection law. In France and some other countries, they have the National Commission on Computing and Freedom, CNIL, which authorises the use of biometric identification only when the purpose of identifying people is to control access of a limited number of people to a well-defined area (real zone, for example a nuclear installation, or virtual zone, for example military servers), whose security interests not only the owner of this area but also the rest of the inhabitants. In addition, the installers of a biometric identifier must guarantee the protection of the data.

In 2000, the CNIL prohibited a student identification system for accessing the dining room at a school in Nice, despite that parents and students agreed to it. The CNIL considered that the security of access to the dining room was not important enough to install an invasive system. In Spain there are several public and private centres, for example swimming pools, which have installed access systems based on fingerprints. Following this line of reasoning, these facilities would not be allowed in France.

Will biometrics be an important factor in our lives in the future? Of course. And that is why citizens must be informed about the most important aspects of biometrics, from the technological, legislative and ethical points of view. Because then they will be able to give their opinions, and their ideas will influence the social changes resulting from the implantation of biometric techniques.

Many articles mark the sad events of 11 September, 2001 as the starting point of the growth of biometrics. It is true that the investment in these techniques reached a major turning point in 2001. The revenues generated by biometric systems went from 400 million dollars that year to 5,000 million in 2010. However, we should not forget that the Scotland Yard fingerprint identification system called Galton-Henry was launched in 1900. And we know that Egyptians used biometric descriptions to identify workers. If biometrics was invented so long ago, why is it talked about so much now? The difference is not only quantitative but qualitative. Because now, if you want to live within society you will be forced to use it. You will not be able to say this does not interest me, because if you do, you will be marginalised from society and you will not have access to any of the services it provides. And for this reason, it must be understood what is a society with biometric technology.

Most states are creating databases with biometric information in order to guarantee the safety of citizens. The FBI manages the fingerprint recognition system called the *Integrated Automated Fingerprint Identification System* that contains 50 million possible criminals with their biometric information and their criminal history. The trend is clear, the databases will grow both in number of individuals and in the volume of information about each individual.

Should we worry about these databases? As the saying goes, information is power, but what information do these databases provide? Do we have to worry that the database has stored that I have a loop-like fingerprint on my index finger? And if they store my DNA? At this point, it is important to distinguish between identity and identification. Identity is the personality of each person, a complex system in permanent construction that extracts its wealth from the multiplicity of its physical, psychological, social and cultural characteristics. Identification is

a set of characters that are unique for each person and assigned in an almost arbitrary manner. We should worry about the storage of our identity but not our identification. Note that when the dictator Franco created the *National Identity Document* (DNI) in 1944, he made a mistake with the name, because what he meant was "Identification". From the information on our fingerprints, we can extract an almost unique identification. But can we determine the identity? In the case of the fingerprint, today it seems difficult, but what about the DNA? Let's not forget the movie *Gattaca* (1997) in which genetic selection is possible so that children are free from illness, which also implies that only genetically correct people can have the best jobs. Will science accumulate the necessary knowledge to reach this social situation? It is not clear, but what is certain is that humanity has a desire for science and that makes us different from other animals and history has shown that it is useless to try to stop it.

The use of biometrics seems to have practical benefits for citizens and the economics of companies. However, the generalisation of biometrics in all fields can be a real danger to the respect for private life. We are currently in a situation that society must be able to solve. Fortunately, independent and international bodies are being created to control the abusive use of biometric information. A specific case is the above mentioned National Commission on Computing and Freedom (CNIL) in France. Science progresses to solve the technical problems that appear. Legislations are adapted to include biometric concepts. When and where will they converge? The challenge is not whether to accept or not accept biometrics but to be able to coexist harmoniously with it.

Summary

In this module we have described the biometric features currently used and the main characteristics that they must have in order to be useful in certain applications. We have seen that not all biometric features can be used in any application. There are biometric features that adapt best to certain types of applications and others that adapt to other types of applications.

We have described the three basic biometric systems: Identification, Verification and Enrolment. We have seen that they have characteristics that distinguish them but they also have some common parts and processes.

The types of real biometric applications have also been described.

We have completed the module by explaining some of the history of biometrics, commenting on films and reflecting on the impact that this science, old but also currently emerging, will have on our society.

Activities

1. **Bertillon method**.
   Take Bertillon measurements of two people, finish filling out the first table (in centimetres). Fill in the second table with the Euclidean distances and decide the maximum value that the Bertillon Threshold must have so that the 4 different people are considered. Now suppose that Will West and William West were really the same person as it was believed at the beginning. What minimum and maximum values should the threshold have?

Bertillon File

Body part	Will West	William West	Person 1	Person 2
Height	178.5	177.5		
Arm span	187.0	188.0		
Seated height	91.2	91.3		
Head length	19.7	19.8		
Head width	15.8	15.9		
Length of right ear	14.8	14.8		
Width of right ear	6.6	6.5		
Length of left foot	28.2	27.5		
Length of left middle finger	12.3	12.2		
Length of left little finger	9.7	9.6		
Length of left forearm	50.2	50.3		

Table of Euclidean distances

Distance	Will West	William West	Person 1	Person 2
Will West	0			
William West		0		
Person 1			0	
Person 2				0

2. **Market revenue**
   What percentage of income does fingerprint recognition provide with respect to other biometric features? And what is the second biometric feature in terms of revenue?
3. **Income in Biometrics**
   The income of biometric systems from 2007 to 2015 (forecast in recent years) in relation to time is a linear function. What is its slope? If the predictions are maintained, what will the income be in 2020?
4. **Verification and Identification**
   Explain the differences between these two systems. When is verification used and when is identification used? The algorithms to compare biometric features can be very time expensive. Therefore, it is usual to use suboptimal algorithms that determine a distance very quickly although it may not be the exact distance. In which cases is it important to use a suboptimal algorithm?
5. **Enrolment**

Explain what enrolment consists in. Normally, in enrolment systems there is someone who checks the data in the entire process of capturing of biometric features. Why is it so important to verify that this process is done correctly?

6. **Processes and systems**
   What are the six processes related to verification, identification and enrolment systems?
7. **Offline and Online**
   Describe a real application that uses an offline system and another application that uses an online system.
8. **Positive and negative searches**
   Explain the difference between the two possible types of searches. Describe a couple of real applications that use these two types of searches.
9. **Biometric features**
   Describe and relate Universality and Particularity.
10. **Biometric features**
    Describe and relate Permanence and Measurability.
11. **Biometric features**
    Describe and relate Performance and Acceptability.
12. **Biometric features**
    Make a table showing all biometric features classified by the part of the body they are located in. Describe their main characteristic and a real application in which this biometric feature could be used.
13. **Biometric features**
    What is the difference between behavioural biometric features and physical biometric features?
14. **Biometric features**
    Study in detail the tables showing the goodness of the biometric features. The evaluations are very suggestive, is there any evaluations that you would change? Keep in mind the comments made after all the tables. What evaluations do you think will be different in 10 years' time?
15. **Application context**
    Describe the types of contexts there are for biometric applications. Give an example of a real application for each option.
16. **Application categories**
    Describe the types of horizontal categories that exist in biometric applications. Give an example of a real application for each option.
17. **Application categories**
    Describe the types of vertical categories that exist in biometric applications.
18. **History of Biometrics**
    When was biometrics first applied to identify people? Explain the first case.
19. **History of Biometrics**
    Do you think the possible cases of biometric features from before the eleventh century are really biometric applications for the identification of people?
20. **History of Biometrics**
    What was Phrenology? Do you think it's a science?
21. **History of Biometrics**
    What was Anthropometry? Do you think it's a science?
22. **History of Biometrics**

Describe the first biometric system that was put into operation. What biometric feature did it use? Was it used to identify or to verify?

23. Reflections on biometrics

Do you think it is correct to apply a biometric system to access a school? And to identify people in conflict or war zones? Do you think there should be a special commission to decide whether or not a biometric system can be implemented? At the state, continental or global level?

Bibliography and References

Books on Biometrics

- Anil K. Jain, Patrick Flynn i Arun A. Ros (editors), “Handbook of Biomtrics”, Editorial Springer, Any 2008, ISBN 978-0-387-71040-2
- David D. Zhang, “Automated Biometrics. Technologies and Systems”, Editorial: Kluweer Academic Publishers, Any 2000, ISBN 0-7923-7856-3
- Anil Jain, Ruud Bolle i Sharath Pankanti, “Biometrics. Personal Identification in Networked Society”, Editorial Kluweer Academic Publishers, Any 1999, ISBN 0-7923-8345-1
- James Wayman, Anil Jain, Davide Maltoni i Dario Maio (editors), “Biometric Systems. Technology, Design and Performance Evaluation”, Editorial Springer, Any 2005, ISBN 1-85233-596-3
- Samir Nanavati, Michael Thieme i Raj Nanavati, “Biometrics. Identity Verification in a Networked World”. Editorial Wiley Computer Publishing, Any 2002, ISBN 0471-09945-7
- Arun A. Ross, Karthik Nandakumar i Anil K. Jain, “Handbook of Multibiometrics”, Springer, Any 2006, ISBN 0-387-22296-0
- H. Li, L. Li & K-A. Toh, “Advanced Topics in Biometrics”, WorldScientific, Any 2011, ISBN: 978-981-4287-84-5

Books on a specific biometric feature

- Anil K. Jain, Patrick Flynn i Arun A. Ros (editors), “Handbook of Biomtrics”, Editorial Springer, Any 2008, ISBN 978-0-387-71040-2
- David D. Zhang, “Automated Biometrics. Technologies and Systems”, Editorial: Kluweer Academic Publishers, Any 2000, ISBN 0-7923-7856-3
- Anil Jain, Ruud Bolle i Sharath Pankanti, “Biometrics. Personal Identification in Networked Society”, Editorial Kluweer Academic Publishers, Any 1999, ISBN 0-7923-8345-1
- James Wayman, Anil Jain, Davide Maltoni i Dario Maio (editors), “Biometric Systems. Technology, Design and Performance Evaluation”, Editorial Springer, Any 2005, ISBN 1-85233-596-3
- Samir Nanavati, Michael Thieme i Raj Nanavati, “Biometrics. Identity Verification in a Networked World”. Editorial Wiley Computer Publishing, Any 2002, ISBN 0471-09945-7
- Arun A. Ross, Karthik Nandakumar i Anil K. Jain, “Handbook of Multibiometrics”, Springer, Any 2006, ISBN 0-387-22296-0
- H. Li, L. Li & K-A. Toh, “Advanced Topics in Biometrics”, WorldScientific, Any 2011, ISBN: 978-981-4287-84-5

Books on pattern recognition

- Richard O. Duda, Peter E. Hart i David G. Stork, “Pattern classification”, Editorial Wiley, Any 2001, ISBN 978-0-471-05669-0
- Tony Jebara, “Machine Learning. Discriminative and Generative”, Editorial Kluweer Academic Publishers, Any 2004, ISBN 1-4020-7647-9
- Elzbieta Pekalska i Robert P. W. Duin, “The Dissimilarity representation for pattern recognition”, Editorial World Scientific, Any 2005, ISBN 981-256-530-2

- Francisco Escolano, Pablo Suau i Boyán Bonev, “Information Theory in Computer Vision and Pattern Recognition”, Editorial Springer, Any 2009, ISBN 978-1-84882-296-2

Books on computer vision

- Richard Szeliski, “Computer vision : algorithms and applications”, Editorial Springer, Any 2011, ISBN 978-1-84882-934-3
- C H Chen, “Handbook of pattern recognition and computer vision”, Editorial Springer, Any 2010, ISBN 978-9-81427-338-1

Acronyms

AFIS: Automatic Fingerprint Identification System.

FVC: Fingerprint Verification Competition.

IVC: Iris Verification Competition.